Cisco IOS XEワイヤレスコントローラソフトウェアにおける不正なユーザ削除の脆弱性

Medium

アドバイザリーID : cisco-sa-ewlc-user-del-hQxMpUDj　CVE-2025-20190
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwm35433

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco IOS XEワイヤレスコントローラソフトウェアのLobby Ambassador Webインターフェイスにおける脆弱性により、認証されたリモート攻撃者が、該当デバイスで定義されている任意のユーザを削除できる可能性があります。

この脆弱性は、ロビーアンバサダーユーザによって実行されるアクションのアクセスコントロールが不十分であることに起因します。攻撃者は、lobby ambassadorユーザアカウントを使用して該当デバイスにログインし、巧妙に細工されたHTTP要求をAPIに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、管理者権限を持つユーザを含め、デバイス上の任意のユーザアカウントを削除できる可能性があります。

注：この脆弱性が不正利用できるのは、攻撃者がlobby ambassadorアカウントのクレデンシャルを取得した場合だけです。このアカウントは、デフォルトでは設定されていません。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-user-del-hQxMpUDj

このアドバイザリは、2025年5月に公開されたCisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）』を参照してください。

該当製品

脆弱性のある製品

公開時点では、次のシスコ製品でCisco IOS XEワイヤレスコントローラソフトウェアの脆弱性のあるリリースを実行し、lobby ambassadorユーザアカウントが有効にされている場合に、この脆弱性の影響を受けました。

- クラウド向け Catalyst 9800-CL ワイヤレスコントローラ
- Catalyst 9300、9400、9500 シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Catalyst 9800 シリーズ ワイヤレス コントローラ
- Catalyst アクセスポイントの組み込みワイヤレスコントローラ

このアドバイザリの公開時点で脆弱性が存在するシスコソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

デバイス設定の確認

Lobby AmbassadorアカウントとHTTPサーバ機能がデバイスに設定されているかどうかを確認するには、次の手順を使用します。

ロビー アンバサダー アカウント設定の確認

デバイスで設定されているlobby ambassadorアカウントの数を確認するには、デバイスにログインしてshow running-config | count type lobby-admin CLIコマンドを実行します。次の例は、1つのLobby Ambassadorアカウントが設定されているデバイスでのCLI出力を示しています。

```
<#root>

Router#

show running-config | count type lobby-admin


Number of lines which match regexp = 1
```

行末の数値は、デバイスで設定されているロビー アンバサダー アカウントの数を示しています。

注：Lobby Ambassadorロールは、RADIUSまたはTACACS+を使用しているユーザアカウントに関連付けることができます。Cisco Identity Services Engine(ISE)などの認証、認可、アカウンティング(AAA)サーバを使用して、デバイスにアクセスするユーザアカウントを管理している場合は、cisco-av-pair=lobby-admin属性が設定されたユーザの存在を確認する必要がありま

す。Cisco ISEでLobby Ambassadorアカウントを設定する方法の例については、「RADIUSおよびTACACS+認証による9800 WLC Lobby Ambassadorの設定」を参照してください。

HTTP サーバ設定の確認

HTTPサーバ機能がデバイスで有効になっているかどうかを確認するには、デバイスにログインし、CLIでshow running-config | include ip http server|secure|activeコマンドを使用して、グローバルコンフィギュレーションにip http serverコマンドまたはip http secure-serverコマンドが存在するかどうかを確認します。どちらかのコマンドが含まれている場合は、HTTP サーバー機能が有効です。

次の例は、HTTPサーバ機能が有効になっているデバイスでのshow running-config | include ip http server|secure|activeコマンドの出力を示しています。

<#root>

```
Router#
show running-config | include ip http server|secure|active


ip http server
ip http secure-server
```

注：デバイス設定にどちらかのコマンドまたは両方のコマンドが含まれている場合は、Web UI機能が有効になっています。

ip http server コマンドが存在し、設定に ip http active-session-modules none が含まれている場合、脆弱性が HTTP 経由でエクスプロイトされることはありません。

ip http secure-serverコマンドが存在し、設定にip http secure-active-session-modules noneも含まれている場合、この脆弱性はHTTPSでは不正利用できません。

Cisco IOS XEワイヤレスコントローラソフトウェアがこの脆弱性の影響を受けるのは、デバイスにlobby ambassadorアカウントが設定されている場合のみです。これはデフォルト設定ではないため、管理者が追加する必要があります。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS ソフトウェア

- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア
- ワイヤレス LAN コントローラ（WLC）AireOS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS および IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。 また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（例：15.9(3)M2、17.3.3）を入力します。
3. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		

Enter release number | Check

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-user-del-hQxMpUDj

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2025年5月7日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。